

**Grupo de trabajo sobre la protección de las personas físicas  
en lo que respecta al tratamiento de datos personales**

**Dictamen 7/99, relativo a**

**el nivel de protección de datos previsto por los principios de «puerto seguro»  
hechos públicos, junto con las preguntas más frecuentes y otros documentos  
relacionados, el 15 y 16 de noviembre de 1999  
por el Departamento de Comercio de los EE.UU.**

**Aprobado el 3 de diciembre de 1999**

## **El Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales**

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995<sup>1</sup>,

Visto el artículo 29 y la letra b) del artículo 30 de la Directiva,

Vistas sus normas de procedimiento y, en particular, sus artículos 12 y 14,

### **Ha aprobado el presente Dictamen 7/99:**

#### **Introducción**

El Grupo de trabajo reafirma su política general sobre la metodología para evaluar la adecuación de la protección de datos en terceros países, resumida en su Documento de trabajo de 24 de julio de 1998 (WP 12: «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE»<sup>2</sup>).

El Grupo de trabajo ha seguido de cerca las conversaciones entre la Comisión y el Departamento de Comercio de los EE.UU., les otorga importancia y considera útil el enfoque de «puerto seguro». Desea contribuir al éxito de los resultados de estas conversaciones y cree que éste dependerá de que se responda a ciertas preocupaciones básicas.

En este contexto, el Grupo de trabajo recuerda que las versiones anteriores de los principios de «puerto seguro» y de las preguntas más frecuentes (FAQ) han sido objeto de los siguientes documentos:

1. Dictamen 1/99 de 26 de enero de 1999 (WP 15)
2. Dictamen 2/99 de 19 de abril de 1999 (WP 19)
3. Dictamen 4/99 de 7 de junio de 1999 (WP 21) y Documento de trabajo de 7 de septiembre de 1999 relativo a algunas de las FAQ (no hecho público)
4. Documento de trabajo de 7 de julio de 1999 (WP 23)

El presente Dictamen hace referencia a la versión más reciente de los principios de «puerto seguro», las FAQ y los documentos relacionados hechos públicos el 15 y el

---

<sup>1</sup> DO L 281 de 23.11.1995, p. 31, disponible en:  
<http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

<sup>2</sup> WP 12 (5025/98): Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. Aprobado el 24 de julio de 1998 (11 lenguas). Se puede consultar en la dirección indicada en la nota 1.

16 de noviembre de 1999<sup>3</sup>. El Grupo de trabajo lamenta que, en un asunto de tanta importancia, se le concediera tan poco tiempo para adoptar su posición. Asimismo, observa que ninguno de los documentos se considera «final» y, por lo tanto, se reserva la posibilidad de cambiar de posición en relación con cualquier modificación posterior de los textos.

El Grupo de trabajo observa que se han logrado algunos avances, pero deplora que, en la última versión de la documentación de EE.UU., únicamente se haya incluido una mínima parte de los comentarios que presentó en documentos anteriores. Por consiguiente, el Grupo de trabajo se reafirma en sus motivos generales de preocupación.

En lo tocante a una posible decisión de adecuación, y teniendo presentes los efectos concretos que tal decisión positiva tendría como punto de referencia para terceros países, el Grupo de trabajo considera que la seguridad jurídica de los principios de «puerto seguro» no debería limitarse a las entidades de los EE.UU., sino que debería abarcar también a las partes interesadas de la UE (responsables de ficheros que deseen transmitir datos a los EE.UU., afectados, autoridades de protección de datos). Desde su Dictamen 1/99, el Grupo de trabajo ha defendido constantemente el punto de vista de que, en lo relativo al fondo, «cualquier conjunto aceptable de principios de "puerto seguro" debe, como requisito mínimo, incluir todos los principios establecidos en las directrices sobre protección de la vida privada (*Privacy guidelines*) de la OCDE, adoptadas entre otros países por Estados Unidos, y que se volvieron a ratificar recientemente en la conferencia de Ottawa de la OCDE» celebrada en octubre de 1998.

### **Alcance y estructura**

El Grupo de trabajo es de la opinión de que los principios de «puerto seguro» están diseñados para controlar el tratamiento de los datos transmitidos a los EE.UU. por responsables de ficheros de la UE. En relación con la recogida de datos personales de los particulares en la UE, el Grupo de trabajo recuerda que normalmente serán de aplicación las disposiciones legislativas nacionales por las que se transpone la Directiva. El Grupo de trabajo recuerda también que el nivel de adecuación establecido en virtud del apartado 6 del artículo 25 de la Directiva únicamente puede hacer referencia a la protección de las personas en relación con el tratamiento de los datos en el tercer país pertinente y no puede afectar al régimen jurídico establecido en la letra c) del artículo 4 de la Directiva.

---

<sup>3</sup> Proyecto de los Principios internacionales de puerto seguro – 15 de noviembre de 1999; Borrador de las preguntas más frecuentes – 15 de noviembre de 1999 (FAQ 1 a 15), Resumen de la Decisión adoptada en virtud del apartado 6 del artículo 25; Carta de David Aaron a John Mogg a la que adjunta los principios de puerto seguro y las FAQ, etc. – 16 de noviembre de 1999; Carta de John Mogg a David Aaron a la que adjunta la Decisión adoptada en virtud del apartado 6 del artículo 25, etc. – 16 de noviembre de 1999.

Los originales en inglés se pueden consultar en: <http://www.ita.doc.gov/td/ecom/menu.htm>

En lo que respecta al «puerto seguro», el Grupo de trabajo recomienda definir de manera clara y sin ambigüedad su alcance tanto para los beneficiarios como para las categorías de transferencias de datos.

Según el cuarto párrafo de los Principios, los beneficios del «puerto seguro» surten efecto desde la fecha en que la entidad que desee acogerse a ellos notifique mediante autocertificación al Departamento Federal de Comercio o a su mandatario su adhesión a los principios. De acuerdo con la FAQ 6, estas cartas de autocertificación se deben enviar como mínimo una vez al año; el Departamento de Comercio (o su representante) «llevará una lista de las entidades que remitan cartas de autocertificación, dispensándoles los beneficios de "puerto seguro". Asimismo, actualizará la lista con las cartas anuales» y las notificaciones relativas a las decisiones de incumplimiento. De conformidad con la FAQ 11, se indicarán en la lista las decisiones negativas contra participantes en el «puerto seguro». A este respecto, el Grupo de trabajo observa lo siguiente:

1. El Departamento de Comercio no efectúa verificaciones previas para determinar si una entidad concreta cumple los criterios de adecuación (adhesión de su política de protección de la vida privada a los principios, jurisdicción de un órgano similar a la FTC para prácticas fraudulentas).
2. El requisito de la autocertificación anual está pensado para mejorar la fiabilidad de la lista; sin embargo, dado que la renovación de dicha autocertificación no es obligatoria, una entidad podría adherirse a los principios durante un año y, a continuación, retirarse del «puerto seguro». Además, existe la posibilidad de que haya impostores no detectados que tarden un periodo significativo en desaparecer de la lista, periodo durante el cual los datos personales continuarían transfiriéndose con normalidad.
3. Las fusiones y absorciones son cada vez más frecuentes en el mundo empresarial en general y, en especial, en los negocios en línea. Es perfectamente posible que una entidad adherida a los principios se fusione o sea absorbida por otra entidad que no pueda o no desee adherirse al «puerto seguro».

En su definición actual, los principios de «puerto seguro» son un sistema voluntario ofrecido a las entidades de EE.UU., basado en la autocertificación (FAQ 6) y la autoevaluación (FAQ 7), respaldado por disposiciones legales en caso de prácticas desleales o fraudulentas. Esto significa que, a menos que se presente e investigue una queja, y hasta el momento en que esto suceda, cualquier entidad de EE.UU. que afirme respetar los beneficios de «puerto seguro» tendría derecho a recibir datos personales de la UE. Teniendo en cuenta los ejemplos anteriores, el Grupo de trabajo insta a la Comisión a analizar métodos para garantizar la protección continua de los datos personales que puedan transmitirse a los siguientes tipos de entidades:

1. Entidades que nunca tendrían que haber aparecido en la lista porque no cumplen los criterios de aceptabilidad.
2. Entidades que, aunque aparecen en la lista, no cumplen los principios.
3. Entidades que, después de estar en la lista durante un año, dejan de estarlo el siguiente, porque no renuevan su autocertificación o porque dejan de ser aceptables en el «puerto seguro».

4. Entidades que, después de aparecer en la lista, son absorbidas por una empresa que no cumple los requisitos de «puerto seguro» (porque no puede o porque no desea adherirse a los principios).

Entre los posibles métodos para garantizar la protección continua, el Grupo de trabajo invita a la Comisión a considerar la eliminación o supresión de los datos transmitidos a una entidad perteneciente a alguna de las categorías anteriores. Además, el Grupo de trabajo desearía recibir aclaraciones en cuanto a la posibilidad de que sigan siendo aplicables las disposiciones sobre prácticas fraudulentas de la *Federal Trade Commission Act* (Ley de la Comisión Federal de Comercio).

Por motivos de seguridad jurídica, el Grupo de trabajo reitera su preocupación por que la lista de beneficiarios sea completamente fiable, actualizada y de fácil acceso público.

En su Documento de trabajo de 7 de julio de 1999, el Grupo de trabajo ya solicitó aclaraciones sobre dos puntos específicos:

- a) Sectores que quedarían excluidos del alcance del «puerto seguro» porque no están dentro de la jurisdicción de un órgano público similar a la FTC (p. ej.: datos de empleados o actividades de carácter no lucrativo).
- b) Actividades que puedan quedar excluidas por la propia entidad adherida al «puerto seguro» gracias a la posibilidad de elección por parte de la empresa.

En relación con el punto **a)**, el Grupo de trabajo concede la máxima importancia a las cartas del Presidente de la FTC, de 23 de septiembre de 1998 y 1 de noviembre de 1999. Estas cartas indican claramente que la jurisdicción de la FTC abarca actos desleales o fraudulentos únicamente si "afectan al comercio o a actividades comerciales". Aparentemente, esto excluye la mayor parte de los datos tratados en relación con una relación laboral (FAQ 9), así como los datos tratados sin propósito comercial (p. ej.: actividades de carácter no lucrativo, investigación). Por tanto, el Grupo de trabajo recomienda que las transmisiones de datos pertenecientes a estas categorías se excluyan expresamente del «puerto seguro».

En cuanto al punto **b)**, el Grupo de trabajo observa que la FAQ 6 invita a las entidades a indicar las «actividades de la entidad cubiertas por su compromiso con los principios de "puerto seguro"». Esto implica que una misma entidad podría tener un pie en el «puerto seguro» y dejar el otro fuera de estos principios. El Grupo de trabajo es de la opinión de que esto crea incertidumbre jurídica (en especial en relación con el uso compartido de los datos dentro de una misma entidad) y solicita que se especifique con urgencia la noción de «actividades».

### **Excepciones y exenciones**

El Grupo de trabajo reitera su preocupación por el hecho de que la adhesión a los principios pueda estar limitada por cualquier «disposición legal o reglamentaria, o jurisprudencia» [letra b) del párrafo 5 de los principios] sin más calificación. Esto se aplica, aparentemente, a las leyes estatales así como a las federales, tanto existentes

como futuras. Para garantizar la seguridad jurídica y la no discriminación en relación con otros niveles adecuación, el Grupo de trabajo recomienda facilitar criterios más precisos y ejemplos concretos para dichas excepciones y limitaciones, así como considerar con la adecuada importancia sus efectos. En cuanto a la necesidad de criterios más precisos, el Grupo de trabajo recomienda distinguir claramente entre opciones y obligaciones: la adhesión a los principios solamente debería limitarse en la medida necesaria para cumplir obligaciones legales o reglamentarias (que, en cualquier caso, prevalecen sobre los principios) pero no como resultado de opciones derivadas de la legislación de EE.UU., dado que esto provocaría un grave menoscabo de los principios.

Por motivos de transparencia y seguridad jurídica, el Grupo de trabajo considera esencial que la Comisión permanezca informada de toda normativa legal o administrativa que pueda influir negativamente en la adhesión a los principios.

En relación con la letra c) del párrafo 5, el Grupo de trabajo recomienda limitar dicho párrafo a las excepciones previstas en la Directiva, que incluyen todas las dispensas permisibles en las normas de Derecho interno de los Estados miembros. En cualquier caso, el Grupo de trabajo es de la opinión de que no se puede invocar ninguna excepción fuera de su contexto específico y que toda excepción se podrá utilizar exclusivamente para servir a su propósito específico.

Para el Grupo de trabajo constituye motivo de preocupación el hecho de que, además de las excepciones antes citadas, las FAQ incluyen una larga lista de excepciones adicionales que, en algunos casos, resultan en la exención de categorías de datos completas; esta afirmación se aplica en concreto a la extensa categoría de «datos de dominio público», que pueden ser «de dominio público» de por sí e independientemente de posibles consideraciones de legitimidad de su tratamiento o de su precisión. El Grupo de trabajo observa que las Directrices de la OCDE no incluyen ninguna exención de este tipo y cree que la aceptación de dicha exención crearía un enorme vacío en la cobertura de la protección de datos.

### **Notificación**

El Grupo de trabajo defiende su punto de vista, reiterado en todos sus Dictámenes anteriores, de que el acuerdo de «puerto seguro» (y especialmente cualquier decisión de adecuación) solamente concierne al tratamiento de datos transmitidos a terceros países por responsables de ficheros establecidos en la UE: los responsables de ficheros establecidos en la UE están sujetos a las disposiciones nacionales de transposición de la Directiva, y esto mismo se aplicaría en circunstancias normales en la recogida de datos personales directamente de los particulares en la UE por una entidad de EE.UU. que recurra a medios, automatizados o no, situados en el territorio de un Estado miembro (artículo 4 de la Directiva).

En la actualidad, todo ello queda aceptado por parte de EE.UU. en la pregunta número 1 de la FAQ 14, relativa a productos médicos y farmacéuticos, y en la FAQ 9 relativa

a datos sobre recursos humanos. No obstante, el principio de Notificación afirma lo siguiente:

*«La notificación se hará (...) la primera vez que se invite a los particulares a proporcionar a la entidad información personal o tan pronto como sea posible».*

La cita anterior implica, o podría malinterpretarse en este sentido, que la recogida de datos de particulares en la UE por una entidad de EE.UU. está regida por los principios de «puerto seguro» y no por las disposiciones nacionales por las que se transpone la Directiva. Así, sus consecuencias irían mucho más allá que el principio de Notificación.

El Grupo de trabajo es de la opinión de que esto no cumple lo dispuesto en la Directiva (artículo 4) y recomienda que la frase citada más arriba sea eliminada y se sustituya por la afirmación clara de los siguientes puntos:

1. Cuando una entidad de EE.UU. tenga la intención de recoger datos personales directamente de particulares de la UE, debe cumplir las disposiciones nacionales de transposición de la Directiva (por ejemplo, los artículos 6, 7, 10, 14 y, cuando sea pertinente, el artículo 8).
2. Cuando el responsable de un fichero establecido en la UE transmita datos personales a la entidad de EE.UU., ésta deberá pedirle que indique los fines para los que se recogieron inicialmente dichos datos (esto es básico para decidir si se ha producido un cambio de los fines después de la transmisión, lo que desencadenaría la aplicación de los principios de Notificación y Opción, y contribuiría a asignar el riesgo y la responsabilidad).

El Grupo de trabajo sugiere que los puntos anteriores sean objeto de una nueva FAQ destinada a esclarecer el principio de Notificación.

Asimismo, el Grupo de trabajo recomienda modificar el principio de Notificación para garantizar que se informe cuando otra entidad haga uso de los datos.

En lo que respecta a la FAQ 4, el Grupo de trabajo observa que no está justificado que los cazatalentos procesen los datos sin el consentimiento de los particulares. Además, se hace referencia a «otras circunstancias en que la aplicación de estos principios perjudicaría los intereses legítimos de la entidad» que el Grupo de trabajo considera una excepción demasiado ambigua.

El Grupo de trabajo hace notar que ha recibido el texto de la FAQ 14 sobre productos médicos y farmacéuticos hace muy poco tiempo y que éste plantea diversas dudas, sobre todo el uso de los datos para fines incompatibles con los relativos a la investigación científica.

## **Opción**

El Grupo de trabajo reitera la opinión expresada en el Documento de trabajo de 7 de julio de 1999: dado que los principios no regulan la legitimidad de los criterios de tratamiento, es necesario reforzar el principio de Opción. En su versión actual, la

combinación de los principios de Notificación y Opción permite utilizar los datos para fines distintos de los notificados sin necesidad de ofrecer la posibilidad de opción (a menos que dichos fines sean incompatibles o que los datos sean delicados), lo que incumple las Directrices de la OCDE («Principio de limitación del uso»)<sup>4</sup>. El Grupo de trabajo apoya la idea de que se debe ofrecer la posibilidad de Opción cuando se utilicen los datos para un fin compatible pero distinto.

El Grupo de trabajo comparte los puntos de vista de la Comisión expresados en la nota a pie de página referida al principio de Opción. Recomienda que la definición de datos delicados se haga coincidir con la Directiva (artículo 8) y considera que la opción únicamente puede ser la base de un tratamiento legítimo si se ha proporcionado la información adecuada.

### **Transferencia ulterior**

El Grupo de trabajo observa con cierta preocupación la adición a este principio de la última frase, que exime totalmente de responsabilidad a las entidades cuando transmitan la información a determinados terceros. Los particulares pueden verse desprotegidos de recursos jurídicos excepto contra la entidad transmisora de los datos, que podría haber actuado de manera imprudente al transmitir la información. El Grupo de trabajo recomienda considerar la posibilidad de reducir la exención de responsabilidad con objeto de mantener la responsabilidad de la entidad transmisora en casos de negligencia e imprudencia y exigir a dicha entidad transmisora que asista al particular en la satisfacción de sus derechos.

### **Seguridad**

El Grupo de trabajo recomienda modificar la FAQ 10 para eliminar la frase relativa a que es innecesaria la presencia en el contrato de cláusulas sobre seguridad, dado que la legislación de diversos Estados miembros exige estas cláusulas en los contratos para el tratamiento dentro del mismo Estado miembro.

### **Integridad de los datos**

El Grupo de trabajo recuerda que, en virtud del párrafo 8 de las Directrices de la OCDE, «los datos deberán ser pertinentes para los fines a los que se destinan y, en la medida necesaria para dichos fines, deberán ser precisos, completos y actualizados». Este principio de «puerto seguro» debería reflejar tal afirmación.

### **Acceso**

El Grupo de trabajo recuerda que el Acceso es un principio fundamental para todo régimen de protección de datos que se precie, puesto que el Acceso es la raíz de la que

---

<sup>4</sup> «Los datos personales no deben divulgarse, ponerse a disposición o utilizarse de ninguna otra forma para fines distintos de los especificados de conformidad con el párrafo 9 (Especificación del fin), con las siguientes excepciones:

- a) con el consentimiento del sujeto de los datos; o bien
- b) cuando lo autorice la ley.»



se derivan todos los derechos del sujeto de los datos, y hace énfasis en que las excepciones a este principio fundamental solamente se permitan en circunstancias excepcionales, al tiempo que reitera la preocupación expresada en todos sus documentos anteriores sobre la amplitud y la ambigüedad de las excepciones y condiciones expresadas por los EE.UU. para el ejercicio de este derecho fundamental.

El Grupo de trabajo vuelve a expresar su opinión de que las consideraciones de coste son pertinentes para decidir las condiciones en que se puede ejercer este derecho, pero no pueden condicionar el propio derecho.

A diferencia de las Directrices de la OCDE<sup>5</sup>, los principios de «puerto seguro» no reconocen el derecho del particular a recibir información «de forma fácilmente inteligible». Además, el principio de Acceso limita el derecho de suprimir a los casos en que los datos sean inexactos (lo que es obvio). En su Dictamen 2/99, el Grupo de trabajo ya ha expresado el punto de vista de que, para que tenga sentido, el derecho de suprimir deberá aplicarse a todos los casos de tratamiento ilícito y que debería incluirse en los principios y no en las FAQ.

La FAQ 8 enumera una larga lista de excepciones al principio de Acceso. El Grupo de trabajo se alegra de que algunas de ellas, en comparación con la versión anterior de la FAQ, se hayan especificado o reducido. Sin embargo, la impresión general es que esta FAQ debilita el principio en lugar de ofrecer orientaciones para su aplicación. En particular, el Grupo de trabajo reitera sus objeciones a la pregunta 2 (noción poco clara) y a la pregunta 7. En cuanto a la pregunta 5, el Grupo de trabajo reafirma su opinión de que las circunstancias para denegar el acceso son demasiado amplias y ambiguas, y que el texto implica que tales consideraciones prevalecen automáticamente sobre el derecho de acceso. Le preocupa que esto dé como resultado un grave debilitamiento del nivel general de protección de los datos.

En lo que respecta a la pregunta 6, el Grupo de trabajo considera inadecuada la redacción del segundo párrafo y recomienda que se elimine o bien que se defina con mayor precisión para limitarlo a eliminar los abusos del derecho de acceso.

El Grupo de trabajo reitera asimismo su oposición a la pregunta 8, por los motivos ya expuestos en el Documento de trabajo de 7 de septiembre de 1999; además, el hecho de que la información sea de dominio público no priva al sujeto de los datos de su derecho de acceso.

### **Aplicación**

El Grupo de trabajo agradece la información detallada de los EE.UU. durante las últimas semanas de conversaciones (en especial: carta de la FTC, comparación de los mecanismos de resolución de litigios sobre protección de la intimidad del sector privado de EE.UU., FAQ 11, Memorándum sobre la *Fair Credit Reporting Act*). Esta información es valiosa y ha permitido al Grupo de trabajo hacerse una idea más global de los instrumentos de aplicación que podrían ponerse a disposición de los sujetos de

---

<sup>5</sup> «Principio de participación individual», punto iv de la letra a).

los datos. Una vez analizada la citada información, el Grupo de trabajo plantea los siguientes motivos de preocupación:

1. Los mecanismos del sector privado existentes abordan exclusivamente las actividades en línea: BBB Online, Web Trust, TRUSTe (el subrayado es nuestro)<sup>6</sup>.
2. Se puede ver un énfasis similar en la carta del Presidente de la FTC de 1 de noviembre de 1999 (párrafo 2: «secreto en línea», «entorno Internet»; párrafo 3: mercado en línea, estudio de sitios web; párrafo 4: «políticas de protección de la intimidad en línea», etc.; el subrayado es nuestro)<sup>7</sup>.
3. Según el párrafo 4 de los principios, también se podrán acoger a los beneficios de «puerto seguro» las entidades sujetas a «*disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones de bolsas nacionales de valores, asociaciones registradas de agentes de valores, organismos de compensación autorizados o comités municipales de regulación de bolsas de valores) que protejan con eficacia el secreto de los datos personales*». No obstante, no se ha facilitado información sobre los organismos públicos que garantizarían la aplicación de esta enorme variedad de disposiciones legales.

En estas circunstancias, el Grupo de trabajo considera que el alcance de las decisiones de adecuación debería restringirse expresamente a los sectores para los que se haya recogido información suficiente y sin ambigüedades y ésta se haya analizado en relación con la existencia de mecanismos de aplicación. De hecho, ampliar el alcance más allá de este límite permitiría recurrir judicialmente la decisión, circunstancia no deseable para ninguna de las partes interesadas.

En relación con el principio de Aplicación, el Grupo de trabajo considera que debe incluir, para que resulte significativo, la indemnización por daños y perjuicios sufridos por los particulares como resultado de la vulneración de los principios: este es el punto de vista general del Grupo de trabajo y se aplica a cualquier tercer país (Documento de trabajo sobre transferencias de datos personales a terceros países; WP 12 de 24 de julio de 1998, página 14: «Reparación adecuada»). Cuando la legislación de los EE.UU. en vigor no establezca la reparación de los daños y perjuicios, la entidad privada debe estar preparada para ofrecer esta posibilidad como condición de adhesión al «puerto seguro».

En la FAQ 11 (resolución de litigios y ejecución), el Grupo de trabajo ha observado que el texto aborda una serie de aspectos relativos a la aplicación que son tan fundamentales que deberían incluirse en el propio principio de Aplicación. Para crear la relación entre los distintos niveles de aplicación, es especialmente importante establecer la norma de que los organismos de resolución de conflictos remitan los asuntos no resueltos a la FTC. También se podrían añadir al principio los requisitos de que los mecanismos de resolución de conflictos sean transparentes y ágiles.

---

<sup>6</sup> Como se indica más arriba, las actividades en línea pueden incluirse en el ámbito de aplicación de la legislación comunitaria cuando conciernen a la recogida de datos personales directamente de los particulares en la UE (véase Alcance y estructura, Notificación).

<sup>7</sup> El mismo comentario que en la nota 6.

Según la FAQ 11, los órganos de resolución de conflictos pueden introducir condiciones de admisibilidad de las quejas. El Grupo de trabajo considera que estas condiciones deberían ser explícitas, objetivas y razonables. Además, la negativa de aceptar a trámite las quejas debe estar debidamente motivada.

En general, el Grupo de trabajo observa que los acuerdos de aplicación en los EE.UU. tienen una estructura muy confusa, en la que no es posible identificar fácilmente los derechos que tienen los ciudadanos en caso de vulneración de los Principios. La FAQ 11 se limita a ofrecer una serie de recomendaciones que pueden dar lugar a una aplicación fragmentada e irregular.

### **FAQ 5: Función de las autoridades de protección de datos**

El Grupo de trabajo ha debatido el texto de la FAQ 5 propuesto por los EE.UU. y su conclusión es que la función de las autoridades de protección de datos descrita en él no es factible práctica ni jurídicamente. En concreto, el Grupo de trabajo observa que la legislación nacional no proporciona a las autoridades nacionales las competencias necesarias para tratar las quejas por infracciones de las normas de protección de datos fuera de su jurisdicción.

Por otra parte, el Grupo de trabajo destaca que las autoridades nacionales están dispuestas a ofrecer su colaboración en forma de información y asesoramiento, si ello puede ser de utilidad en el marco del «puerto seguro». Entiende que los EE.UU. han intentado lograr esta colaboración durante un periodo limitado tras el lanzamiento del «puerto seguro».

En este contexto, el Grupo de trabajo invita a la Comisión a que investigue si esta oferta de información y asesoramiento, más el compromiso unilateral de la entidad de EE.UU. de que seguirá los consejos de las autoridades nacionales (compromiso que, en caso de incumplimiento, daría lugar a acciones de la FTC por fraude), podría ayudar a satisfacer los requisitos de la letra a) del principio de Aplicación del «puerto seguro». En caso afirmativo, observa que las autoridades nacionales podrían estar preparadas para colaborar en este sentido durante un periodo inicial de tres años. Además, el Grupo de trabajo indica que las autoridades nacionales desearían revisar este compromiso antes del fin de dicho periodo si el número de entidades de EE.UU. que eligen esta opción es tal que se concluya sin duda que este método se emplea como sustituto de los acuerdos adecuados de aplicación en los EE.UU., y no como un medio provisional para cubrir un vacío limitado.<sup>8</sup>

El Grupo de trabajo también invita a la Comisión a investigar la función que podría ejercer un mecanismo a escala europea que, entre otros aspectos, podría facilitar un foro que ayudara a garantizar un enfoque coordinado y armonizado.

---

<sup>8</sup> Algunas delegaciones indicaron que se reservan su postura respecto a este párrafo.

## Proyecto de Decisión de la Comisión (de 24 de noviembre de 1999)

El Grupo de trabajo desea llamar la atención de la Comisión sobre los siguientes puntos:

1. No hay ninguna referencia al trabajo llevado a cabo por el Grupo de trabajo a fin de establecer los criterios para evaluar la adecuación en terceros países (WP 12). En opinión del Grupo de trabajo, la evaluación debería realizarse sobre estos criterios para garantizar un enfoque equilibrado y ecuaníme en todos los países, independientemente de que sigan un enfoque legislativo o normativo para la protección de los datos. Además, debería incluir una referencia específica a los dictámenes emitidos por el Grupo de trabajo sobre el «puerto seguro» en los EE.UU., así como a sus lugares de publicación.
2. En cuanto al fondo de la Decisión, el Grupo de trabajo observa que los criterios de adhesión al «puerto seguro» no son los mismos en los textos de EE.UU. que en el proyecto de Decisión. Según los párrafos iniciales 3 y 4 de los Principios publicados por los EE.UU., las entidades pueden adherirse al «puerto seguro» por los siguientes métodos:

- «a) integrándose en un programa de protección de la vida privada elaborado por el sector privado que siga los principios,*
- b) elaborando sus propias medidas de protección de la vida privada, siempre que se adecuen a dichos principios,*
- c) estando sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra, que protejan con eficacia el secreto de los datos personales.»*

En virtud del artículo 1 del proyecto de Decisión de la Comisión, se consideran pertenecientes al «puerto seguro» las entidades que:

*«hayan manifestado de forma pública su compromiso de cumplir los Principios y queden bajo la jurisdicción de un organismo público independiente facultado para investigar las quejas y solicitar medidas provisionales contra las prácticas desleales o fraudulentas.»*

Es necesario que los Principios se correspondan con la Decisión.

3. Asimismo, el Grupo de trabajo observa que el considerando 8 establece que la jurisdicción de la *Federal Trade Commission* está sujeta a diversas exclusiones legales. Sin embargo, no se indican expresamente los sectores excluidos ni tampoco se afirma que todos ellos estén cubiertos por otro organismo público. Igualmente, debería incluirse una referencia a las disposiciones por las que se faculta al reducido número de organismos públicos mencionados para actuar contra las prácticas fraudulentas o desleales.

Dado que, para las entidades que deseen adherirse al «puerto seguro», es una condición *sine qua non* estar sujetas a la jurisdicción de un organismo público facultado para actuar contra las prácticas desleales o fraudulentas, el Grupo de

trabajo considera fundamental esclarecer este punto y que el alcance del «puerto seguro» se limite a los sectores regidos por un organismo público de este tipo.

4. El proyecto de Decisión de la Comisión no menciona la manera en que las entidades pueden verse privadas de los beneficios de «puerto seguro»; dicho de manera más sencilla, los procedimientos para su eliminación de la lista del Departamento de Comercio.

El único compromiso del texto de EE.UU. es indicar en la lista *«toda notificación que reciba de los organismos de resolución de litigios, autorregulación y/o de la administración sobre cualquier incumplimiento sistemático de los principios o de las resoluciones de los organismos mencionados que haya sido cometido por entidades del puerto seguro. No obstante, se concederá un plazo de 30 días para notificar este extremo a dichas entidades así como la oportunidad de alegar».* (FAQ 11)

Según el proyecto de Decisión, esta indicación negativa por parte del Departamento de Comercio de los EE.UU. únicamente puede dar lugar a la suspensión de las transmisiones de datos en virtud de la letra a) del apartado 2 del artículo 2. En la actualidad, aunque se suspenda la transmisión de datos a una entidad en virtud de la letra a) del apartado 2 del artículo 2, esta suspensión no quedaría reflejada porque la lista de EE.UU. no mostrará las decisiones de adecuación negativas tomadas en la UE. Sin embargo, es necesario garantizar que los operadores de la UE pueden confiar en la lista.

Además, en opinión del Grupo de trabajo, las condiciones establecidas en el apartado 2 del artículo 2<sup>9</sup> para la suspensión de los flujos de datos podrían ser difíciles de cumplir en la práctica, lo que sería inaceptable cuando se están vulnerando los derechos de la persona. Para solucionar este aspecto, las palabras «perjuicio irreparable» del apartado 2 del artículo 2 deberían sustituirse por «perjuicio grave e inminente».

5. El Grupo de trabajo observa que el apartado 3 del artículo 1 incluye el siguiente texto propuesto por los Estados Unidos: *«Se considerará que el cumplimiento de la Fair Credit Reporting Act o la Financial Modernization Act estadounidenses garantizan un nivel adecuado de protección, si las actividades de una entidad*

---

<sup>9</sup> Apartado 2 del artículo 2: «Las autoridades competentes de los Estados miembros podrán además ejercer su competencia de suspender los flujos de datos hacia una entidad que suscriba los Principios, para proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes:

- a) el organismo público de los EE.UU. mencionado en la letra b) del apartado 1 del artículo 1 o el mecanismo independiente de recurso de los EE.UU. mencionado en la letra a) del Principio de Aplicación resuelven que se han vulnerado los principios
- b) existen razones para creer que el mecanismo estadounidense de aplicación no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión, existen grandes probabilidades de que se estén vulnerando los Principios y las autoridades competentes del Estado miembro han hecho esfuerzos razonables para notificárselo a la entidad y proporcionarle la oportunidad de alegar

y la continuación de la transferencia provocaría un perjuicio irreparable a los afectados. La suspensión cesará en cuanto se cumplan los Principios.»

*entran en el ámbito de aplicación de una de ambas leyes».* En relación con estas leyes de EE.UU., el Grupo de trabajo llama la atención de la Comisión sobre el hecho de que en el orden del día de la 17ª reunión del 7 de junio se incluyó un análisis de la *Fair Credit Reporting Act*, pero no hubo tiempo de analizar dicha ley ni de evaluar su nivel de adecuación. En lo que respecta a la *Financial Modernization Act*, el Grupo de trabajo recibió su texto en fechas demasiado recientes.

A la luz de lo anterior, el Grupo de trabajo solamente podrá emitir un dictamen sobre el nivel de adecuación de ambas leyes después de haberlas analizado detalladamente. Mientras no haya una decisión sobre la adecuación de estas leyes, deberá eliminarse de la Decisión toda referencia a las mismas.

6. El Grupo de trabajo también considera que en el apartado 1 del artículo 2 debe incluirse la siguiente modificación:

«El artículo 1 se entenderá sin perjuicio de las facultades de las autoridades competentes de los Estados miembros para emprender acciones destinadas a garantizar el cumplimiento de las disposiciones nacionales adoptadas en virtud de disposiciones distintas a los artículos 25 y 26 de la Directiva.»

### **Canje de notas**

*(sin fecha, pero incluidas en el sitio web el 15 de noviembre)*

El Grupo de trabajo desea llamar la atención de la Comisión sobre los siguientes aspectos:

1. **El denominado periodo de gracia o fecha de entrada en vigor:** Tanto el proyecto de carta de los EE.UU. como el proyecto de respuesta de la Comisión incluyen fórmulas al efecto de que la Comisión y los Estados miembros utilizarán la flexibilidad del artículo 26 para evitar interrupciones en los flujos de datos hacia las entidades de los EE.UU. durante un periodo determinado de conformidad con la decisión del apartado 6 del artículo 25 sobre el marco del «puerto seguro». Esto proporcionará a las entidades de los EE.UU. la oportunidad de decidir si desean adherirse al «puerto seguro» y, en caso necesario, adaptar sus prácticas de información a los requisitos del «puerto seguro».

Teniendo en cuenta que, de conformidad con la Directiva, la Comisión solamente podrá actuar en relación con transferencias de datos a países terceros en los siguientes casos: a) un tercer país no garantiza un nivel de protección adecuado y la Comisión inicia negociaciones destinadas a remediar la situación (apartados 4, 5 y 6 del artículo 25), o b) cuando la Comisión decida que determinadas cláusulas contractuales tipo ofrecen garantías suficientes (apartado 4 del artículo 26), el Grupo de trabajo se pregunta en qué se piensa basar la Comisión para utilizar la flexibilidad del artículo 26 de la Directiva a fin de otorgar a las entidades de los EE.UU. tiempo suficiente para decidir si desean o no adherirse al «puerto seguro».

2. **Utilización de los contratos - Decisiones tomadas en virtud del artículo 26:** En el proyecto de carta de los EE.UU. se afirma lo siguiente: «*La Comisión y los Estados miembros consideran que los principios (de «puerto seguro» de los EE.UU.) pueden utilizarse en estos acuerdos para las disposiciones materiales sobre protección de datos... La Comisión ha iniciado conversaciones con los Estados miembros en el Comité del artículo 31... para adoptar una decisión en virtud del apartado 4 del artículo 26 que autorice, cuando proceda, los acuerdos tipo...»*

Teniendo en cuenta que el Grupo de trabajo siempre ha sostenido que el análisis de la adecuación de las soluciones contractuales exige tomar en consideración un conjunto de cuestiones más amplio que el abordado en las soluciones marco, un compromiso de este tipo sería prematuro. No es preciso resaltar que en primer lugar se deben mejorar los principios de «puerto seguro» hasta que se consideren adecuados y solamente después podrá considerarse su inclusión en el contenido de los contratos tipo.

### **Conclusiones**

En vista de las observaciones y recomendaciones anteriores, el Grupo de trabajo concluye que los acuerdos de «puerto seguro» propuestos, tal como quedan reflejados en las versiones actuales de los diversos documentos, continúan siendo insatisfactorios. El Grupo de trabajo invita a la Comisión a que inste a la parte estadounidense a realizar una serie de mejoras clave, en particular las siguientes:

- Especificar el alcance del «puerto seguro» y, en especial, eliminar todo posible malentendido referido a que las entidades de EE.UU. pueden optar por basarse en los principios de «puerto seguro» en circunstancias en las que es de aplicación la propia Directiva.
- Facilitar acuerdos más fiables que permitan identificar con seguridad a los participantes en el «puerto seguro» y evitar el riesgo de continuar otorgándoles los beneficios del «puerto seguro» cuando, por un motivo u otro, hayan sido eliminados de la lista.
- Afirmar sin ningún asomo de duda que todos los participantes en el «puerto seguro» están sujetos a la jurisdicción de un organismo público con las facultades apropiadas para controlar su aplicación.
- Establecer la norma de que los organismos de resolución de conflictos del sector privado deben remitir las quejas no resueltas a uno de estos organismos públicos.
- Eliminar las generalizaciones y ambigüedades de las excepciones y exenciones permitidas, de manera que las excepciones sean precisamente eso, es decir, que se apliquen solamente cuando sea necesario y en la medida requerida, y que no sean invitaciones generales para hacer caso omiso de los principios. Esto cobra especial importancia en relación con el derecho de acceso.
- Reforzar el principio de Opción, que es el elemento decisivo del enfoque de los EE.UU.

Estos puntos se han desarrollado con mayor detalle en las secciones anteriores del presente Dictamen y el Grupo de trabajo desearía que se tomaran en cuenta las consideraciones pertinentes.

Además, el Grupo de trabajo invita a la Comisión a revisar el artículo 2 del proyecto de Decisión para indicar claramente que ésta no afectará las facultades de aplicación de las autoridades nacionales competentes en lo que respecta a las disposiciones por las que se transpone la Directiva a las legislaciones nacionales, con excepción de sus artículos 25 y 26, así como para permitir la posibilidad de intervenir de conformidad con el apartado 2 del artículo 2 cuando puedan existir perjuicios «graves e inminentes» para los particulares en caso de no intervención.

Por último, el Grupo de trabajo destaca la importancia de continuar e incluso acelerar el trabajo sobre las cláusulas de los contratos tipo, con el objeto de tomar una o varias decisiones en virtud del apartado 4 del artículo 26, lo que constituye una parte importante de la simplificación y transparencia de las salvaguardias necesarias para la transmisión a zonas en las que no hay otros medios de garantizar la protección adecuada.

Hecho en Bruselas, a 3 de diciembre de 1999

Por el Grupo de trabajo

*El Presidente*

Peter J. HUSTINX